View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Finite Fields and Their Applications 16 (2010) 243–254

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A class of constacyclic codes over $\mathbb{Z}_{p^m}$ ☆

Shixin Zhu [a,b], Xiaoshan Kai [a,b,*]

[a] School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, PR China
[b] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, PR China

ARTICLE INFO

Article history:
Received 22 May 2009
Revised 26 March 2010
Available online 10 April 2010
Communicated by W. Cary Huffman

MSC:
94B05
94B60

Keywords:
Constacyclic codes
Galois rings
Generator polynomials
Discrete Fourier transform

ABSTRACT

We study $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of an arbitrary length, where λ is a unit of $\mathbb{Z}_{p^m}$ and $m \geqslant 2$ is a positive integer. We first derive the structure of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m, a)$ and determine the Hamming and homogeneous distances of such constacyclic codes. These codes are then used to classify all $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p). In particular, the Gray images of $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ are also discussed.
© 2010 Elsevier Inc. All rights reserved.

1. Introduction

Codes over finite rings have been studied since the early 1970s. After the discovery that certain good nonlinear binary codes can be constructed from cyclic codes over $\mathbb{Z}_4$ via the Gray map [10], codes over finite rings have received much more attention. In particular, constacyclic codes over finite rings have been a topic of study (see, for example, [2–4,6,11,13–19]). In [16,17], Wolfmann studied negacyclic codes over $\mathbb{Z}_4$ of odd length and gave some important results about such negacyclic codes. Tapia-Recillas and Vega generalized these results to the setting of codes over $\mathbb{Z}_{2^k}$ in [14]. Later, Ling and Blackford extended most of the results in [14,16,17] to the ring $\mathbb{Z}_{p^{k+1}}$ in [11], where some constacyclic codes over $\mathbb{Z}_{p^{k+1}}$ were characterized. More generally, the structure of negacyclic codes of length n over a finite chain ring R such that the length n is not divisible by the characteristic p of the

☆ The research is supported by the National Natural Science Foundation of China (No. 60973125), College Doctoral Funds of China (No. 20080359003) and HFUT Research Grant (No. 081003F).
* Corresponding author at: School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, PR China.
E-mail addresses: zhushixin@hfut.edu.cn (S. Zhu), kxs6@sina.com (X. Kai).

1071-5797/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2010.03.003

residue field $\bar{R}$ was obtained by Dinh and López-Permouth in [6]. The situation when the code length n is divisible by the characteristic p of the residue field $\bar{R}$ yields the so-called repeated-root codes. In recent years, several classes of repeated-root constacyclic codes over finite rings have been studied extensively (see, for examples, [2–4,6,13,18,19]). Using a transform approach, Blackford [2] classified all negacyclic codes over $\mathbb{Z}_4$ of even length and generalized Wolfmann's results [16,17] to negacyclic codes of even length. Sălăgean [13] showed that negacyclic codes of even length over the Galois ring $GR(2^a, m)$ are principally generated. In [4], Dinh studied the structure of λ-constacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$ where λ is any unit of $\mathbb{Z}_{2^a}$ with form $4k-1$, and established the Hamming, homogeneous, Lee, and Euclidean distances of all such constacyclic codes.

In this paper, we investigate $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of an arbitrary length, where λ is a unit of $\mathbb{Z}_{p^m}$ and $m \geqslant 2$ is a positive integer. The class of constacyclic codes over $\mathbb{Z}_{p^m}$ includes the following two classes of codes as special cases: (i) when $p=2$ the class of constacyclic codes coincides with the class of λ-constacyclic codes over $\mathbb{Z}_{2^a}$ where λ is any unit of $\mathbb{Z}_{2^a}$ with form $4k-1$ (cf. [4]); (ii) when $m=2$ and $\lambda = p-1$ the class of constacyclic codes coincides with the class of $(1-p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ (cf. [11]). Using the discrete Fourier transform, we classify all $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length $p^s n$, where $\gcd(n, p) = 1$ and $s \geqslant 0$ is an integer. The rest of this paper is organized as follows. Section 2 gives some notations and results about constacyclic codes and Galois rings. In Section 3, we study the structure of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m, a)$ and determine the Hamming and homogeneous distances of all such constacyclic codes. In Section 4, we classify all $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) using the discrete Fourier transform. Section 5 deals with $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ and their images under a generalization of the Gray map.

2. Preliminaries

Let R be a finite commutative ring with identity. An ideal I of the ring R is called *principal* if it is generated by one element. If R has a unique maximal ideal, then R is a *local ring*; if the ideals of R are linearly ordered, then R is a *finite chain ring*. The ring R is a finite chain ring if and only if R is a local ring and its maximal ideal is principal. Examples of finite chain rings include $\mathbb{Z}_{p^m}$ and Galois rings. The following results are well-known facts about finite chain rings (cf. [12]).

Proposition 2.1. *Let R be a finite commutative chain ring with maximal ideal M and residue field $\bar{R}$. Let ν be a fixed generator of M and t the nilpotency index of ν. Then we have*

(i) *the distinct proper ideals of R are $\langle \nu^i \rangle$, $i = 1, 2, \dots, t-1$;*
(ii) *for $i = 0, 1, \dots, t$, $|\langle \nu^i \rangle| = |\bar{R}|^{t-i}$.*

A polynomial $f(x)$ in $\mathbb{Z}_{p^m}[x]$ is said to be a *basic irreducible polynomial* if its reduction modulo p, denoted by $\bar{f}(x)$, is irreducible in $\mathbb{Z}_p[x]$. Define the Galois ring $GR(p^m, a) = \mathbb{Z}_{p^m}[x]/\langle h(x) \rangle$, where $h(x)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^m}[x]$ of degree a. The Galois ring $GR(p^m, a)$ is local with maximal ideal $\langle p \rangle$ and residue field $\mathbb{F}_{p^a}$. The polynomial $h(x)$ can be chosen so that $\xi = x + \langle h(x) \rangle$ is a primitive $(p^a - 1)$st root of unity. The set $\mathcal{T}_a = \{0, 1, \xi, \dots, \xi^{p^a-2}\}$ is a complete set of coset representatives modulo $\langle p \rangle$ and is called the *Teichmüller set*, which can be viewed as the set of all solutions to the polynomial $x^{p^a} - x$ over $GR(p^m, a)$. Each element $r \in GR(p^m, a)$ can be written uniquely as

$$r = \xi_0 + p\xi_1 + p^2\xi_2 + \cdots + p^{m-1}\xi_{m-1},$$

where $\xi_i \in \mathcal{T}_a$, $0 \leqslant i \leqslant m-1$. According to the following proposition, r is an invertible element in $GR(p^m, a)$ if and only if $\xi_0 \neq 0$.

Proposition 2.2. *Let R be a finite commutative ring with identity. If $x - y$ is nilpotent in R, then x is a unit if and only if y is a unit.*

The set $\mathcal{T}_a$ is mapped onto $\mathbb{F}_{p^a}$ under the canonical reduction map (modulo p reduction) from $GR(p^m, a)$ to $\mathbb{F}_{p^a}$. Under the representation above, the Frobenius automorphism σ on $GR(p^m, a)$ acts as follows

$$\sigma(r) = \xi_0^p + p\xi_1^p + p^2\xi_2^p + \cdots + p^{m-1}\xi_{m-1}^p.$$

The map σ is an automorphism of $GR(p^m, a)$, fixes only elements of $\mathbb{Z}_{p^m}$, and generates the group of automorphisms of $GR(p^m, a)$, which is cyclic of order a.

Hensel's lemma [12, Theorem XIII.4] is an important tool in studying finite commutative chain rings, which guarantees that factorizations into a product of pairwise coprime polynomials in $\mathbb{Z}_p[x]$ lift to such factorizations over $\mathbb{Z}_{p^m}$. If $\gcd(n, p) = 1$, then the polynomial $x^n - 1$ factors uniquely into monic basic irreducible polynomials in $\mathbb{Z}_{p^m}[x]$ as $x^n - 1 = f_1(x) f_2(x) \cdots f_r(x)$. Let a be the order of p modulo n. Then $\mathbb{F}_{p^a}$ contains a primitive nth root of unity. By Hensel's lemma, $GR(p^m, a)$ also has a primitive nth root ξ of unity. For each j, $0 \leqslant j \leqslant n-1$, there exists a unique i, $1 \leqslant i \leqslant r$, such that $f_i(\xi^j) = 0$, and $f_i(x)$ is called the *minimal polynomial* of ξ^j over $\mathbb{Z}_{p^m}$.

For a finite commutative ring R, a code over R of length N is a nonempty subset of R^N, and a code over R of length N is linear if it is an R-submodule of R^N. For some fixed unit ω of R, the ω-constacyclic shift τ_ω on R^N is the shift $\tau_\omega(c_0, c_1, \ldots, c_{N-1}) = (\omega c_{N-1}, c_0, \ldots, c_{N-2})$, and a linear code C of length N over R is ω-constacyclic if the code is invariant under the ω-constacyclic shift τ_ω. Note that the R-module R^N is isomorphic to the R-module $R[x]/\langle x^N - \omega\rangle$. We identify a codeword $c = (c_0, c_1, \ldots, c_{N-1})$ with its polynomial representation $c(x) = c_0 + c_1 x + \cdots + c_{N-1}x^{N-1}$. Then $xc(x)$ corresponds to an ω-constacyclic shift of $c(x)$ in the ring $R[x]/\langle x^N - \omega\rangle$. Thus ω-constacyclic codes of length N over R can be identified as ideals in the ring $R[x]/\langle x^N - \omega\rangle$.

Throughout this paper, let p be a prime number and λ a unit of $\mathbb{Z}_{p^m}$, and let $N = p^s n$ with $\gcd(n, p) = 1$ and s being a nonnegative integer.

3. $(1 + \lambda p)$-Constacyclic codes of length p^s over $GR(p^m, a)$

3.1. Structure

We denote $\mathcal{R}(a) = GR(p^m, a)[x]/\langle x^{p^s} - (1 + \lambda p)\rangle$. $(1 + \lambda p)$-Constacyclic codes of length p^s over $GR(p^m, a)$ are precisely the ideals of $\mathcal{R}(a)$.

Lemma 3.1. *The element $x - 1$ is nilpotent in $\mathcal{R}(a)$.*

Proof. In $\mathcal{R}(a)$, we have

$$\begin{aligned}(x-1)^{p^s} &= x^{p^s} + (-1)^{p^s} + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} x^{p^s-i} \\ &= 1 + (-1)^{p^s} + \lambda p + \sum_{i=1}^{p^s-1} (-1)^i \binom{p^s}{i} x^{p^s-i}. \end{aligned} \tag{1}$$

Since $\binom{p^s}{i} \equiv 0 \pmod{p}$ for $1 \leqslant i \leqslant p^s - 1$, there exists a polynomial $f(x) \in GR(p^m, a)[x]$ such that $(x-1)^{p^s} = pf(x)$, which implies $(x-1)^{p^s m} = 0$. Thus, $x - 1$ is nilpotent in $\mathcal{R}(a)$. $\square$

Let

$$\mu : GR\big(p^m, a\big) \to \mathbb{F}_{p^a}, \quad \mu(r) = r \pmod{p}$$

denote the canonical reduction map from $GR(p^m,a)$ to $\mathbb{F}_{p^a}$. The map μ extends naturally to a map from $GR(p^m,a)[x]$ to $\mathbb{F}_{p^a}[x]$. Each element $r \in GR(p^m,a)$ can be uniquely written as $r = r_0 + r_1 p + r_2 p^2 + \cdots + r_{m-1} p^{m-1}$ with $r_i \in \mathcal{T}_a$. We simply write $\mu(r) = r_0$.

Lemma 3.2. *Let $a(x) \in \mathcal{R}(a)$. Then*

(i) *$a(x)$ can be uniquely written as*

$$a(x) = a_0 + a_1(x-1) + a_2(x-1)^2 + \cdots + a_{p^s-1}(x-1)^{p^s-1} \tag{2}$$

where $a_i \in GR(p^m,a)$, $0 \leqslant i \leqslant p^s-1$;

(ii) *$a(x)$ is a unit in $\mathcal{R}(a)$ if and only if $\mu(a_0) \neq 0$.*

Proof. (i) is obvious. (ii) Note that $a(x)$ can be expressed as $a(x) = \mu(a_0) + pr + (x-1)g(x)$, for some $r \in GR(p^m,a)$ and $g(x) \in \mathcal{R}(a)$. Write $f(x) = pr + (x-1)g(x)$, then $f(x) = a(x) - \mu(a_0)$. Since $x-1$ and p are nilpotent in $\mathcal{R}(a)$, it follows that $(x-1)g(x)$ and $ph(x)$ are nilpotent in $\mathcal{R}(a)$. Therefore, $f(x)$ is nilpotent in $\mathcal{R}(a)$. By Proposition 2.2, $a(x)$ is a unit in $\mathcal{R}(a)$ if and only if $\mu(a_0)$ is a unit; if and only if $\mu(a_0) \neq 0$. □

Lemma 3.3. *In $\mathcal{R}(a)$ we have $(x-1)^{p^s} = p\rho(x)$, where $\rho(x)$ is a unit in $\mathcal{R}(a)$. Thus, the nilpotency index of $x-1$ is $p^s m$.*

Proof. Write $f(x) = \sum_{i=1}^{p^s-1}(-1)^i\binom{p^s}{i}x^{p^s-i}$. Expanding $f(x)$ in $(x-1)$, we get

$$f(x) = \sum_{i=1}^{p^s-1}\sum_{j=0}^{p^s-i}(-1)^i\binom{p^s}{i}\binom{p^s-i}{j}(x-1)^{p^s-i-j}. \tag{3}$$

The constant term of (3) is $f(1) = \sum_{i=1}^{p^s-1}(-1)^i\binom{p^s}{i} = -1-(-1)^{p^s}$. Hence, $f(x)$ can be represented as $f(x) = f(1) + p\sum_{i=1}^{p^s-1} b_i(x-1)^i$, where $b_i \in GR(p^m,a)$ for $1 \leqslant i \leqslant p^s-1$. From (1), we have

$$(x-1)^{p^s} = p\left(\lambda + \sum_{i=1}^{p^s-1} b_i(x-1)^i\right).$$

By Lemma 3.2(ii), $\rho(x) = \lambda + \sum_{i=1}^{p^s-1} b_i(x-1)^i$ is a unit in $\mathcal{R}(a)$ since λ is a unit in $GR(p^m,a)$. This completes the proof. □

Theorem 3.4. *The ring $\mathcal{R}(a)$ is a chain ring with maximal ideal $\langle x-1\rangle$ and residue field $\mathbb{F}_{p^a}$, and the nilpotency index of $x-1$ is $p^s m$. The ideals of $\mathcal{R}(a)$ are $\langle (x-1)^i\rangle$, $0 \leqslant i \leqslant p^s m$.*

Proof. Let $r(x)$ be any element in $\mathcal{R}(a)$. Then $r(x)$ can be expressed as $r(x) = r_0 + pr + (x-1)g(x)$, where $r_0 \in \mathcal{T}_a$, $r \in GR(p^m,a)$, and $g(x) \in \mathcal{R}(a)$. If $r_0 = 0$, then $r(x) = pr + (x-1)g(x)$. By Lemma 3.3, $p = (x-1)^{p^s}[\rho(x)]^{-1}$, hence $r(x) = (x-1)h(x)$ for some polynomial $h(x) \in \mathcal{R}(a)$. This gives $r(x) \in \langle x-1\rangle$. If $r_0 \neq 0$, then $r(x)$ is a unit in $\mathcal{R}(a)$. Therefore, for any element $r(x)$ in $\mathcal{R}(a)$, either $r(x)$ is a unit, or $r(x) \in \langle x-1\rangle$. This implies that $\mathcal{R}(a)$ is local with maximum ideal $\langle x-1\rangle$. According to [6, Proposition 2.1], $\mathcal{R}(a)$ is a chain ring whose ideals are $\langle (x-1)^i\rangle$, $0 \leqslant i \leqslant p^s m$. □

Corollary 3.5. *Let C be a $(1+\lambda p)$-constacyclic code of length p^s over $GR(p^m,a)$. Then $C = \langle (x-1)^i\rangle \subseteq \mathcal{R}(a)$, for some $i \in \{0,1,\ldots,p^s m\}$, and the number of codewords in C is $|C| = p^{a(p^s m-i)}$.*

Proof. Since $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m,a)$ are precisely the ideals of $\mathcal{R}(a)$, we have the first result. The second result follows from the fact that $\mathcal{R}(a)$ is a finite chain ring with residue field $\mathbb{F}_{p^a}$ (cf. Proposition 2.1). □

3.2. Hamming and homogeneous distances

Using the linear ordering of some classes of constacyclic codes over finite rings or fields, Dinh computed various kinds of distances of such constacyclic codes in [3–5]. In the following, we use this technique to compute the Hamming distance of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m,a)$. Let $C_i=\langle (x-1)^i\rangle$ be a nonzero $(1+\lambda p)$-constacyclic code of length p^s over $GR(p^m,a)$, for some $i\in\{0,1,\dots,p^sm-1\}$. Denote the Hamming distance of C_i by $d_H(C_i)$. Since $\langle 1\rangle = C_0\supset C_1\supset\cdots\supset C_{p^sm-1}$, it follows that $d_H(C_{p^sm-1})\geqslant d_H(C_{p^sm-2})\geqslant\cdots\geqslant d_H(C_1)\geqslant d_H(C_0)=1$.

Proposition 3.6. *For $0\leqslant i\leqslant p^s(m-1)$, $C_i=\langle (x-1)^i\rangle\subseteq\mathcal{R}(a)$ has Hamming distance $d_H(C_i)=1$.*

Proof. By Lemma 3.3, $C_{p^s(m-1)}=\langle (x-1)^{p^s(m-1)}\rangle=\langle p^{m-1}\rangle$. Hence, $d_H(C_{p^s(m-1)})=1$, which implies $d_H(C_i)=1$ for $0\leqslant i\leqslant p^s(m-1)$. □

For $p^s(m-1)+1\leqslant i\leqslant p^sm-1$, let $i=p^s(m-1)+t$ with $1\leqslant t\leqslant p^s-1$, then $C_i=\langle (x-1)^{p^s(m-1)+t}\rangle=\langle p^{m-1}(x-1)^t\rangle$. Thus, each code C_i is the cyclic code $\langle (x-1)^t\rangle$ of length p^s over $\mathbb{F}_{p^a}$ multiplied by p^{m-1}. Combining this with [5, Theorem 6.4], we obtain the Hamming distance of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m,a)$ as follows.

Theorem 3.7. *Let $C_i=\langle (x-1)^i\rangle$ be a nonzero $(1+\lambda p)$-constacyclic code of length p^s over $GR(p^m,a)$, for some $i\in\{0,1,\dots,p^sm-1\}$. Then the Hamming distance $d_H(C_i)$ of C_i is given by*

$$d_H(C_i)=\begin{cases}1, & \text{if } 0\leqslant i\leqslant p^s(m-1),\\ \beta+2, & \text{if } p^s(m-1)+\beta p^{s-1}+1\leqslant i\leqslant p^s(m-1)+(\beta+1)p^{s-1}\\ & \text{where } 0\leqslant\beta\leqslant p-2,\\ (t+1)p^k, & \text{if } p^sm-p^{s-k}+(t-1)p^{s-k-1}+1\leqslant i\leqslant p^sm-p^{s-k}+tp^{s-k-1}\\ & \text{where } 1\leqslant t\leqslant p-1, \text{ and } 1\leqslant k\leqslant s-1.\end{cases}$$

The homogeneous weight for finite chain rings was defined in [9], where the concept of the Gray map between ($\mathbb{Z}_4$, Lee distance) and ($\mathbb{Z}_2^2$, Hamming distance) was extended to the context of finite chain rings. We recall the definitions for homogeneous weight and homogeneous distance for codes over $GR(p^m,a)$.

Definition 3.8. The homogeneous weight on $GR(p^m,a)$ is a weight function on $GR(p^m,a)$ given as

$$w_{\text{hom}}:GR\big(p^m,a\big)\to\mathbb{N},\quad r\mapsto\begin{cases}(p^a-1)p^{a(m-2)}, & \text{if } r\in GR(p^m,a)\backslash\langle p^{m-1}\rangle,\\ p^{a(m-1)}, & \text{if } r\in\langle p^{m-1}\rangle\backslash\{0\},\\ 0, & \text{if } r=0.\end{cases}$$

The homogeneous weight of a codeword $c=(c_0,c_1,\dots,c_{n-1})$ over $GR(p^m,a)$ is the rational sum of the homogeneous weights of its components. The homogeneous distance $d_{\text{hom}}(C)$ of a linear code C is the smallest homogeneous weight of its nonzero codewords. Now we compute the homogeneous distance of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m,a)$.

Theorem 3.9. *Let $C_i=\langle (x-1)^i\rangle$ be a nonzero $(1+\lambda p)$-constacyclic code of length p^s over $GR(p^m,a)$, for some $i\in\{0,1,\dots,p^sm-1\}$. Then the homogeneous distance $d_{\text{hom}}(C_i)$ of C_i is given by*

$$d_{\mathrm{hom}}(C_i) = \begin{cases} (p^a-1)p^{a(m-2)}, & \text{if } 0 \leqslant i \leqslant p^s(m-2), \\ p^{a(m-1)}, & \text{if } p^s(m-2)+1 \leqslant i \leqslant p^s(m-1), \\ (\beta+2)p^{a(m-1)}, & \text{if } p^s(m-1)+\beta p^{s-1}+1 \leqslant i \leqslant p^s(m-1)+(\beta+1)p^{s-1} \\ & \text{where } 0 \leqslant \beta \leqslant p-2, \\ (t+1)p^{a(m-1)+k}, & \text{if } p^s m - p^{s-k}+(t-1)p^{s-k-1}+1 \leqslant i \leqslant p^s m - p^{s-k}+tp^{s-k-1} \\ & \text{where } 1 \leqslant t \leqslant p-1, \text{ and } 1 \leqslant k \leqslant s-1. \end{cases}$$

Proof. By Lemma 3.3, $C_{p^s(m-2)} = \langle (x-1)^{p^s(m-2)} \rangle = \langle p^{m-2} \rangle$. If $0 \leqslant i \leqslant p^s(m-2)$, then $\langle 1 \rangle = C_0 \supseteq C_i \supseteq C_{p^s(m-2)} = \langle p^{m-2} \rangle$. Hence, $d_{\mathrm{hom}}(C_i) = (p^a-1)p^{a(m-2)}$.

If $p^s(m-2)+1 \leqslant i \leqslant p^s(m-1)$, then $\langle p^{m-2}(x-1) \rangle = C_{p^s(m-2)+1} \supseteq C_i \supseteq C_{p^s(m-1)} = \langle p^{m-1} \rangle$. Let $C' = \langle p^{m-2}(x-1) \rangle \setminus \langle p^{m-1} \rangle$. Suppose that C' has a codeword $c(x)$ of Hamming weight 1. Then $c(x)$ can be expressed as $p^{m-2}\eta x^q$, where η is a unit in $GR(p^m,a)$ and $0 \leqslant q \leqslant p^s-1$. Since ηx^q is invertible in $\mathcal{R}(a)$, we have $p^{m-2} \in \langle p^{m-2}(x-1) \rangle$. This gives $\langle p^{m-2} \rangle \subseteq \langle p^{m-2}(x-1) \rangle$, a contradiction. Hence, C' has no codewords of Hamming weight 1. Note that $2(p^a-1)p^{a(m-2)} \geqslant p^{a(m-1)}$ for positive integers $a \geqslant 1$ and $m \geqslant 2$, so $d_{\mathrm{hom}}(C_{p^s(m-2)+1}) = p^{a(m-1)}$. Also, $d_{\mathrm{hom}}(C_{p^s(m-1)}) = p^{a(m-1)}$. Thus, $d_{\mathrm{hom}}(C_i) = p^{a(m-1)}$.

The third and fourth cases follow from Theorem 3.7 and the fact that each component of codewords in $C_i = \langle (x-1)^i \rangle$ with $p^s(m-1)+1 \leqslant i \leqslant p^s m - 1$ has the form ξp^{m-1}, where $\xi \in \mathcal{T}_a$. □

4. $(1+\lambda p)$-Constacyclic codes of length $p^s n$ over $\mathbb{Z}_{p^m}$

Recall that $N = p^s n$ with $\gcd(n,p)=1$, where $s \geqslant 0$ is an integer and p is a prime number. We denote $\mathcal{R}_N = \mathbb{Z}_{p^m}[x]/\langle x^N - (1+\lambda p) \rangle$, so $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length N are precisely the ideals of $\mathcal{R}_N$. We introduce the quotient ring $GR(p^m,a)[u]/\langle u^{p^s} - (1+\lambda p) \rangle$, which can be obtained from $\mathcal{R}(a)$ by substituting the variable u for x. For convenience, we still denote it by $\mathcal{R}(a)$. If $a=1$, then $\mathcal{R}(1) = \mathbb{Z}_{p^m}[u]/\langle u^{p^s} - (1+\lambda p) \rangle$. We just write $\mathcal{R}$ for $\mathcal{R}(1)$. Note that $(1+\lambda p)^{p^{m-1}} \equiv 1 \pmod{p^m}$ by induction on m, so $u^{p^{s+m-1}} = 1$ in $\mathcal{R}$. There exists a natural $\mathbb{Z}_{p^m}$-module isomorphism $\varphi : \mathcal{R}^n \to \mathbb{Z}_{p^m}^N$ defined by

$$\begin{aligned} &\varphi\big(c_{0,0} + c_{0,1}u + \cdots + c_{0,p^s-1}u^{p^s-1}, \ldots, c_{n-1,0} + c_{n-1,1}u + \cdots + c_{n-1,p^s-1}u^{p^s-1}\big) \\ &\quad = (c_{0,0}, c_{1,0}, \ldots, c_{n-1,0}, c_{0,1}, c_{1,1}, \ldots, c_{n-1,1}, \ldots, c_{0,p^s-1}, c_{1,p^s-1}, \ldots, c_{n-1,p^s-1}). \end{aligned}$$

We have that

$$\begin{aligned} &\varphi\left(u\left(\sum_{j=0}^{p^s-1} c_{n-1,j}u^j\right), \sum_{j=0}^{p^s-1} c_{0,j}u^j, \ldots, \sum_{j=0}^{p^s-1} c_{n-2,j}u^j\right) \\ &\quad = \big((1+\lambda p)c_{n-1,p^s-1}, c_{0,0}, c_{1,0}, \ldots, c_{n-2,p^s-1}\big). \end{aligned}$$

This gives that a constacyclic shift by u in $\mathcal{R}^n$ corresponds to a $(1+\lambda p)$-constacyclic shift in $\mathbb{Z}_{p^m}^N$. Thus, $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) correspond to u-constacyclic codes over $\mathcal{R}$ of length n via the map φ.

4.1. *Discrete Fourier transform*

It is well known that the discrete Fourier transform (DFT) is an important tool to better understand linear codes. Repeated-root cyclic and negacyclic codes over finite rings were studied using the discrete Fourier transform in [1,2,7,8,19]. Next, we use this transform approach to classify $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ for a given length.

Let a be the order of p modulo n, and I a complete set of p-cyclotomic coset representatives modulo n. Let $cl_p(h,n)$ be the p-cyclotomic coset modulo n containing h, and a_h the size of this coset. Let ξ be a primitive nth root of unity in $GR(p^m,a)$.

Definition 4.1. Let $\mathbf{c}=(c_{0,0},\dots,c_{n-1,0},c_{0,1},\dots,c_{n-1,1},\dots,c_{0,p^s-1},\dots,c_{n-1,p^s-1})\in\mathbb{Z}_{p^m}^N$, with $c(x)=\sum_{i=0}^{n-1}\sum_{j=0}^{p^s-1}c_{i,j}x^{i+jn}$ the corresponding polynomial. The discrete Fourier transform of $c(x)$ is the vector

$$(\hat{c}_0,\hat{c}_1,\dots,\hat{c}_{n-1})\in\mathcal{R}(a)^n,$$

with $\hat{c}_h=c(u^{n'}\xi^h)=\sum_{i=0}^{n-1}\sum_{j=0}^{p^s-1}c_{i,j}u^{n'i+j}\xi^{hi}$, for $0\leqslant h\leqslant n-1$, where $nn'\equiv 1 \pmod{p^{s+m-1}}$. Define the Mattson–Solomon polynomial of $\mathbf{c}$ to be $\hat{c}(z)=\sum_{h=0}^{n-1}\hat{c}_{n-h}z^h$ (here $\hat{c}_n=\hat{c}_0$).

The following lemma shows that a vector of $\mathbb{Z}_{p^m}^N$ can be recovered from its discrete Fourier transform.

Lemma 4.2 *(Inversion formula). Let $\mathbf{c}\in\mathbb{Z}_{p^m}^N$ with $\hat{c}(z)$ its Mattson–Solomon polynomial as defined above. Then*

$$\mathbf{c}=\varphi\left[\left(1,u^{-n'},u^{-2n'},\dots,u^{-(n-1)n'}\right)*\frac{1}{n}\left(\hat{c}(1),\hat{c}(\xi),\dots,\hat{c}\left(\xi^{n-1}\right)\right)\right]$$

where $*$ denotes componentwise multiplication.

Proof. Let $0\leqslant t\leqslant n-1$. Then

$$\begin{aligned}\hat{c}\left(\xi^t\right)&=\sum_{h=0}^{n-1}\hat{c}_h\xi^{-ht}=\sum_{h=0}^{n-1}\left(\sum_{i=0}^{n-1}\sum_{j=0}^{p^s-1}c_{i,j}u^{n'i+j}\xi^{hi}\right)\xi^{-ht}\\&=\sum_{i=0}^{n-1}\sum_{j=0}^{p^s-1}c_{i,j}u^{n'i+j}\sum_{h=0}^{n-1}\xi^{h(i-t)}\\&=\left(nu^{n't}\right)\sum_{j=0}^{p^s-1}c_{t,j}u^j.\end{aligned}$$

Hence, $u^{-n't}(1/n)\hat{c}(\xi^t)=\sum_{j=0}^{p^s-1}c_{t,j}u^j$. By the definition of the map φ, the result easily follows from a straightforward computation. □

For each element $r\in GR(p^m,a)$ expressed as $r=\xi_0+p\xi_1+p^2\xi_2+\cdots+p^{m-1}\xi_{m-1}$, where $\xi_i\in\mathcal{T}_a$, recall that the Frobenius automorphism σ on $GR(p^m,a)$ is given by $\sigma(r)=\xi_0^p+p\xi_1^p+p^2\xi_2^p+\cdots+p^{m-1}\xi_{m-1}^p$. We can extend the Frobenius automorphism σ to $\mathcal{R}(a_h)$ by setting $\sigma(u)=u$. It is easy to verify that $\hat{c}_h\in\mathcal{R}(a_h)$ and $\hat{c}_{ph}=\sigma(\hat{c}_h)$ where subscripts are calculated modulo n. Now let $\mathcal{C}=\{(\hat{c}_0,\hat{c}_1,\dots,\hat{c}_{n-1})\in\mathcal{R}(a)^n \mid \hat{c}_h\in\mathcal{R}(a_h),\ \hat{c}_{ph}=\sigma(\hat{c}_h)\}$. We make $\mathcal{C}$ a ring via componentwise addition and multiplication. It is easy to verify that $\mathcal{C}\cong\bigoplus_{h\in I}\mathcal{R}(a_h)$.

Theorem 4.3. *Let $N=p^sn$ with $\gcd(n,p)=1$, and let I be a complete set of p-cyclotomic coset representatives modulo n. Then*

$$\gamma: \quad \mathcal{R}_N \to \bigoplus_{h\in I} \mathcal{R}(a_h)$$

defined by $\gamma(c(x)) = (\hat{c}_h)_{h\in I}$ is a ring isomorphism. In particular, if C is a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length N, then C is isomorphic to $\bigoplus_{h\in I} C_h$, where C_h is the ideal $\{c(u^{n'}\xi^h) \mid c(x) \in C\} \subseteq \mathcal{R}(a_h)$.

Proof. Define the map $\gamma : \mathcal{R}_N \to \mathcal{C}$, where $\gamma(c(x)) = (\hat{c}_0, \hat{c}_1, \ldots, \hat{c}_{n-1})$. Let $a(x), b(x)$ be polynomials over $\mathbb{Z}_{p^m}$ of degree less than N. Then there exist $q(x), r(x) \in \mathbb{Z}_{p^m}[x]$ such that $a(x)b(x) = q(x)(x^N - (1+\lambda p)) + r(x)$, where $\deg(r(x)) < N$. So we have $a(u^{n'}\xi^h)b(u^{n'}\xi^h) = r(u^{n'}\xi^h)$, which means $\gamma(a(x)b(x)) = \gamma(a(x)) * \gamma(b(x))$, where $*$ denotes the componentwise product. Clearly, $\gamma(a(x)+b(x)) = \gamma(a(x)) + \gamma(b(x))$. If $\gamma(c(x)) = \mathbf{0}$, then from the Inversion Formula we have $\sum_{j=0}^{p^s-1} c_{t,j}u^j = 0$ for any $0 \leqslant t \leqslant n-1$. This gives $c(x) = 0$, and hence γ is an injection. Also, $|\mathcal{C}| = \prod_{h\in I} p^{a_h m p^s} = p^{mN}$, which means that γ is a bijection. Thus, γ is an isomorphism. $\square$

From Theorems 3.4 and 4.3, we immediately get the following enumeration result.

Corollary 4.4. *The number of distinct $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) is $(p^s m + 1)^t$, where t is the number of p-cyclotomic cosets modulo n.*

Remark. The ideals $\langle 0\rangle, \langle 1\rangle, \langle p\rangle, \ldots, \langle p^{m-1}\rangle$ of $GR(p^m, a)$ can be identified as the ideals $\langle (u-1)^m\rangle$, $\langle (u-1)^0\rangle, \langle (u-1)^1\rangle, \ldots, \langle (u-1)^{m-1}\rangle$ of $GR(p^m, a)[u]/\langle u-(1+\lambda p)\rangle$, respectively. This allows $s = 0$ in Theorem 4.3.

4.2. Generator polynomials

Now we describe a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) in terms of its generator polynomials. First we give the following lemma.

Lemma 4.5. *Let n' be a positive integer such that $nn' \equiv 1 \pmod{p^{s+m-1}}$, and let $f_h(x)$ be the minimal polynomial of ξ^h over $\mathbb{Z}_{p^m}$ for each $h \in I$. Then*

(i) *$f_h(u^{n'}\xi^i)$ is a unit in $\mathcal{R}(a_i)$ if $i \notin cl_p(h,n)$;*
(ii) *$f_h(u^{n'}\xi^h) \in \langle u-1\rangle$ but $f_h(u^{n'}\xi^h) \notin \langle (u-1)^2\rangle$.*

Proof. (i) Since $f_h(x) = \prod_{l\in cl_p(h,n)}(x-\xi^l)$, it follows that

$$f_h\left(u^{n'}\xi^i\right) = \prod_{l\in cl_p(h,n)} \left(u^{n'}\xi^i - \xi^l\right) = \prod_{l\in cl_p(h,n)} \left[\left(u^{n'}-1\right)\xi^i + \left(\xi^i - \xi^l\right)\right].$$

If $i \notin cl_p(h,n)$, then $\xi^i - \xi^l \neq 0$. Note that

$$\left(u^{n'}-1\right)\xi^i = (u-1)\left(u^{n'-1} + u^{n'-2} + \cdots + 1\right)\xi^i,$$

and so $(u^{n'}-1)\xi^i$ is noninvertible. Hence, $f_h(u^{n'}\xi^i)$ is a unit if $i \notin cl_p(h,n)$.

(ii) As $x^n - 1 = \prod_{i\in I} f_i(x)$, we have $\prod_{i\in I} f_i(u^{n'}\xi^h) = (u^{n'}\xi^h)^n - 1 = u-1$. From (i) we know that $f_i(u^{n'}\xi^h)$ is a unit in $\mathcal{R}(a_h)$ for $i \neq h$. Hence $f_h(u^{n'}\xi^h) = q(u)(u-1)$, where $q(u)$ is a unit in $\mathcal{R}(a_h)$. This gives $f_h(u^{n'}\xi^h) \in \langle u-1\rangle$. Suppose that $f_h(u^{n'}\xi^h) \in \langle (u-1)^2\rangle$. Then there exists $g(u) \in GR(p^m, a_h)[u]$ such that $f_h(u^{n'}\xi^h) = g(u)(u-1)^2$. Hence $q(u)(u-1) = g(u)(u-1)^2$. This implies $u-1 \in \langle (u-1)^2\rangle$, which means $\langle u-1\rangle \subseteq \langle (u-1)^2\rangle$. This is a contradiction. Therefore, $f_h(u^{n'}\xi^h) \notin \langle (u-1)^2\rangle$. $\square$

Theorem 4.6. *Let C be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p). Then $C = \langle \prod_{j=0}^{p^s m} [g_j(x)]^j \rangle$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^m}[x]$ (some of the $g_j(x)$'s may be 1).*

Proof. By Theorem 4.3, $C \cong \bigoplus_{h\in I} C_h$, where C_h is the ideal $\{c(u^{n'}\xi^h) \mid c(x) \in C\}$ in $\mathcal{R}(a_h)$. For each $0 \leqslant j \leqslant p^s m$, we define $g_j(x)$ to be the product of all minimal polynomials of ξ^h such that $C_h = \langle (u-1)^j \rangle$. If $c(x) = r(x)\prod_{j=0}^{p^s m} [g_j(x)]^j \in C$ for some polynomial $r(x) \in \mathcal{R}_N$, then $c(u^{n'}\xi^h) = r(u^{n'}\xi^h)\prod_{j=0}^{p^s m} [g_j(u^{n'}\xi^h)]^j \in \mathcal{R}(a_h)$. By Lemma 4.5, $c(u^{n'}\xi^h) \in \langle (u-1)^j \rangle$, but $c(u^{n'}\xi^h) \notin \langle (u-1)^{j-1} \rangle$. Thus, we can take $g(x) = \prod_{j=0}^{p^s m} [g_j(x)]^j$ as the generator polynomial of C. □

Corollary 4.7. *If $C = \langle \prod_{j=0}^{p^s m} [g_j(x)]^j \rangle$ is a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p), where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^m}[x]$, then $|C| = p^t$, where $t = \sum_{j=0}^{p^s m} (p^s m - j)\deg(g_j(x))$.*

Proof. By Theorem 4.3, the size of C is $\prod_{h\in I} |C_h|$, where C_h is the ideal of $\mathcal{R}(a_h)$. If $C_h = \langle (u-1)^j \rangle$, then $g_j(\xi^h) = 0$. By Corollary 3.5, $|C_h| = p^{a_h(p^s m - j)}$. Calculating the product, we get the result. □

4.3. Hamming distance

Lemma 4.8. *Let C be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) with generator polynomial $\prod_{j=0}^{p^s m} [g_j(x)]^j$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^m}[x]$. Then $C \cap \langle p^{m-1} \rangle = \langle p^{m-1} \prod_{j=1}^{p^s} [g_{j+p^s(m-1)}(x)]^j \rangle$.*

Proof. For each $h \in I$, note that the ideal $\langle p^{m-1} \rangle$ in $\mathcal{R}_N$ corresponds to the ideal $\langle p^{m-1} \rangle = \langle (u-1)^{p^s(m-1)} \rangle$ in $\mathcal{R}(a_h)$ under the map γ. By the proof of Theorem 4.6, we have

$$\langle p^{m-1} \rangle = \langle (x^n - 1)^{p^s(m-1)} \rangle = \langle [g_0(x)g_1(x)\cdots g_{p^s m}(x)]^{p^s(m-1)} \rangle \subseteq \mathcal{R}_N.$$

Therefore, $C \cap \langle p^{m-1} \rangle = \langle p^{m-1} \prod_{j=1}^{p^s} [g_{j+p^s(m-1)}(x)]^j \rangle$. □

Recall that $\bar{c}(x) \equiv c(x) \pmod p$. Let $C = \langle \prod_{j=0}^{p^s m} [g_j(x)]^j \rangle$ be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p), where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^m}[x]$. We define $C^* = \{\bar{h}(x) \mid p^{m-1}h(x) \in C\}$. We also define $\widetilde{C} = \langle \prod_{j=1}^{p^s} [\bar{g}_{j+p^s(m-1)}(x)]^j \rangle$, which is a cyclic code over $\mathbb{Z}_p$ of length $N = p^s n$ (n prime to p).

Theorem 4.9. *Let C be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^m}$ of length $N = p^s n$ (n prime to p) with generator polynomial $\prod_{j=0}^{p^s m} [g_j(x)]^j$, where $g_j(x)$'s are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^m}[x]$. Let $\widetilde{C} = \langle \prod_{j=1}^{p^s} [\bar{g}_{j+p^s(m-1)}(x)]^j \rangle$ be the cyclic code over $\mathbb{Z}_p$ of length $N = p^s n$ (n prime to p). Then $d_H(C) = d_H(\widetilde{C})$.*

Proof. We first prove $\widetilde{C} = C^*$. Let $\bar{c}(x)$ be any element in C^*. Then $p^{m-1}c(x) \in C$. By Lemma 4.8, we have $p^{m-1}c(x) \in C \cap \langle p^{m-1} \rangle = \langle p^{m-1} \prod_{j=1}^{p^s} [g_{j+p^s(m-1)}(x)]^j \rangle$. This gives

$$\bar{c}(x) = \bar{d}(x) \prod_{j=1}^{p^s} [\bar{g}_{j+p^s(m-1)}(x)]^j \in \widetilde{C},$$

for some $\bar{d}(x) \in \mathbb{Z}_p[x]$. Hence, $C^* \subseteq \widetilde{C}$. On the other hand, for any $b(x) \in \widetilde{C}$,

$$b(x) = \bar{e}(x) \prod_{j=1}^{p^s} \left[\bar{g}_{j+p^s(m-1)}(x)\right]^j,$$

for some $\bar{e}(x) \in \mathbb{Z}_p[x]$. Since $p^{m-1}e(x) \prod_{j=1}^{p^s} [g_{j+p^s(m-1)}(x)]^j \in C \cap \langle p^{m-1} \rangle$, we have $b(x) \in C^*$. It follows that $\widetilde{C} \subseteq C^*$, and so $\widetilde{C} = C^*$. For any nonzero codeword $c(x) \in C$, $p^{m-1}c(x) \in C$ and $w_H(p^{m-1}c(x)) \leqslant w_H(c(x))$, hence it is sufficient to compute the Hamming distance of $C \cap \langle p^{m-1} \rangle$ so as to obtain the Hamming distance of C. Note that for any $f(x) \in \mathbb{Z}_{p^m}$, $f(x)$ and $p^{m-1} f(x)$ have nonzero coefficients exactly in those positions where $f(x)$ has unit coefficients, so $w_H(p^{m-1} f(x)) = w_H(\bar{f}(x))$. Thus $d_H(C) = d_H(\widetilde{C})$. $\square$

5. $(1 + \lambda p)$-Constacyclic codes of length $p^s n$ over $\mathbb{Z}_{p^2}$

In this section, we work over the ring $\mathbb{Z}_{p^2}$. In [11], Ling and Blackford gave a necessary and sufficient condition for a $(1 - p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ to be linear, and established the Gray image of a $(1 - p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ for length relatively prime to p in many cases. Now, we determine the homogeneous distance of some $(1 + \lambda p)$-constacyclic codes over $\mathbb{Z}_{p^2}$ of length $N = p^s n$ (n prime to p) using their residue and torsion codes. We first give a Gray map from $\mathbb{Z}_{p^2}^N$ to $\mathbb{Z}_p^{pN}$, which is a special case of the Gray isometries in [9,11].

To avoid confusion, we denote additions in $\mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^2}^N$, and $\mathbb{Z}_{p^2}[x]$ by $+$, while additions in $\mathbb{Z}_p$, $\mathbb{Z}_p^N$, $\mathbb{Z}_p^{pN}$ and $\mathbb{Z}_p[x]$ are denoted by $\oplus$. Every element $x \in \mathbb{Z}_{p^2}$ can be written uniquely as $x = r_0(x) + pr_1(x)$, where $r_i(x) \in \{0, 1, \ldots, p-1\}$. The Gray map ϕ: $\mathbb{Z}_{p^2} \to \mathbb{Z}_p^p$ is defined as $\phi(x) = (a_0, a_1, \ldots, a_{p-1})$, where $a_\epsilon = r_1(x) \oplus \epsilon r_0(x)$, for $0 \leqslant \epsilon \leqslant p-1$. We can extend the Gray map ϕ from $\mathbb{Z}_{p^2}^N$ to $\mathbb{Z}_p^{pN}$ as follows: for $\mathcal{A} = (A_0, A_1, \ldots, A_{N-1}) \in \mathbb{Z}_{p^2}^N$, let $\phi(\mathcal{A}) = (a_0, a_1, \ldots, a_{pN-1})$, where $a_{\epsilon N+j} = r_1(A_j) \oplus \epsilon r_0(A_j)$, for $0 \leqslant \epsilon \leqslant p-1$ and $0 \leqslant j \leqslant N-1$.

Take $a = 1$ and $m = 2$ in Definition 3.8, and we get the homogeneous weight on $\mathbb{Z}_{p^2}$:

$$w_{\text{hom}}(r) = \begin{cases} p-1, & \text{if } r \in \mathbb{Z}_{p^2} \backslash \langle p \rangle, \\ p, & \text{if } r \in \langle p \rangle \backslash \{0\}, \\ 0, & \text{if } r = 0. \end{cases}$$

For any $\mathcal{A}, \mathcal{B} \in \mathbb{Z}_{p^2}^N$, the homogeneous distance d_{hom} is given by $d_{\text{hom}}(\mathcal{A}, \mathcal{B}) = w_{\text{hom}}(\mathcal{A} - \mathcal{B})$. The Gray map ϕ is a distance-preserving map from $(\mathbb{Z}_{p^2}^N, d_{\text{hom}})$ to $(\mathbb{Z}_p^{pN}, d_H)$ (cf. [11, Proposition 2.2]). A code over $\mathbb{Z}_{p^2}$ of length N with M codewords and homogeneous distance d is an (N, M, d) code. For a linear code C over $\mathbb{Z}_{p^2}$ of length N, we can associate to the code C two linear codes over $\mathbb{Z}_p$ of length N. The residue code $\text{Res}(C) = \{x \in \mathbb{Z}_p^N \mid \exists y \in \mathbb{Z}_p^N \mid x + py \in C\}$ and the torsion code $\text{Tor}(C) = \{x \in \mathbb{Z}_p^N \mid px \in C\}$. The reduction modulo p from C to $\text{Res}(C)$ is given by $\mu(x) = x \pmod p$. Clearly, the map μ is a ring homomorphism with $\operatorname{Ker}\mu \cong \text{Tor}(C)$. Hence, by the First Isomorphism theorem of finite groups, we have $|C| = |\text{Res}(C)||\text{Tor}(C)|$. In the following, we give the residue and torsion codes of a $(1 + \lambda p)$-constacyclic code over $\mathbb{Z}_{p^2}$ of length $N = p^s n$ (n prime to p). Obviously, they are both cyclic codes over $\mathbb{Z}_p$ of length $N = p^s n$ (n prime to p), that is, they are the ideals in $\bar{\mathcal{R}} = \mathbb{Z}_p[x]/\langle x^N - 1 \rangle$. We abbreviate f for $f(x)$ when the context is clear.

Lemma 5.1. *Let f be a monic divisor of $x^n - 1$ in $\mathbb{Z}_p[x]$. Then, in $\bar{\mathcal{R}}$, $\langle f^{p^s+l} \rangle = \langle f^{p^s} \rangle$, for any positive integer l.*

Proof. Let $\hat{f} = (x^n - 1)/f$. Since f and $\hat{f}$ are coprime in $\mathbb{Z}_p[x]$, it follows that f^l and $\hat{f}^{p^s}$ are coprime in $\mathbb{Z}_p[x]$ for any positive integer l. Therefore, there exist $\theta, \vartheta \in \mathbb{Z}_p[x]$ such that $\theta f^l + \vartheta \hat{f}^{p^s} = 1$ in $\mathbb{Z}_p[x]$. Computing in $\bar{\mathcal{R}}$, we have

$$\begin{aligned} \theta f^{p^s+l} &= \left(1 - \vartheta \hat{f}^{p^s}\right) f^{p^s} \\ &= f^{p^s} - \vartheta \left(x^n - 1\right)^{p^s} \\ &= f^{p^s}. \end{aligned}$$

Consequently, $\langle f^{p^s+l}\rangle = \langle f^{p^s}\rangle$ for any positive integer l. $\square$

Lemma 5.2. *Let C be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^2}$ of length $N = p^s n$ (n prime to p) with generator polynomial $\prod_{j=0}^{2p^s} g_j^j$, where g_j's are monic coprime divisors of $x^n - 1$ in $\mathbb{Z}_{p^2}[x]$. Then*

(i) $\mathrm{Res}(C) = \langle \bar{g}_1 \bar{g}_2^2 \cdots \bar{g}_{p^s-1}^{p^s-1} (\bar{g}_{p^s} \cdots \bar{g}_{2p^s})^{p^s}\rangle$;
(ii) $\mathrm{Tor}(C) = \langle \prod_{j=1}^{p^s} \bar{g}_{j+p^s}^j \rangle$.

Proof. It is obvious that $\mathrm{Res}(C) = \langle \prod_{j=0}^{2p^s} \bar{g}_j^j\rangle \subseteq \bar{\mathcal{R}}$. By Lemma 5.1,

$$\mathrm{Res}(C) = \left\langle \bar{g}_1 \bar{g}_2^2 \cdots \bar{g}_{p^s-1}^{p^s-1} (\bar{g}_{p^s} \cdots \bar{g}_{2p^s})^{p^s}\right\rangle.$$

This gives part (i). Let $D = \langle \prod_{j=1}^{p^s} \bar{g}_{j+p^s}^j \rangle \subseteq \bar{\mathcal{R}}$. As in the proof of Lemma 4.8,

$$\langle p\rangle = \left\langle \left(x^n - 1\right)^{p^s}\right\rangle = \left\langle (g_0 g_1 \cdots g_{2p^s})^{p^s}\right\rangle \subseteq \mathbb{Z}_{p^2}[x]/\left\langle x^N - (1+\lambda p)\right\rangle.$$

So there exists an invertible element $r \in \mathbb{Z}_{p^2}[x]/\langle x^N - (1+\lambda p)\rangle$ such that $p = r(g_0 g_1 \cdots g_{2p^s})^{p^s}$. It follows that $p \prod_{j=1}^{p^s} \bar{g}_{j+p^s}^j = r(g_0 g_1 \cdots g_{p^s})^{p^s} \prod_{j=1}^{p^s} g_{j+p^s}^{j+p^s} \in C$. Hence, $D \subseteq \mathrm{Tor}(C)$. From Corollary 4.7 and $|C| = |\mathrm{Res}(C)||\mathrm{Tor}(C)|$, we can compute $|D| = |\mathrm{Tor}(C)|$. Therefore, $\mathrm{Tor}(C) = \langle \prod_{j=1}^{p^s} \bar{g}_{j+p^s}^j \rangle$. $\square$

Theorem 5.3. *Let C be a $(1+\lambda p)$-constacyclic code over $\mathbb{Z}_{p^2}$ of length $N = p^s n$ (n prime to p), and let d_1 and d_2 be the minimum Hamming distances of the residue and torsion codes, respectively. If $(p-1)d_1 \geqslant pd_2$, then the minimum homogeneous distance of C is pd_2.*

Proof. For any nonzero codeword $c \in C$ whose entries have the units of $\mathbb{Z}_{p^2}$, reduction modulo p must be in $\mathrm{Res}(C)$. So $w_{\mathrm{hom}}(c) \geqslant (p-1)d_1$. On the other hand, note that $p\,\mathrm{Tor}(C)$ is contained in C. Hence, if $(p-1)d_1 \geqslant pd_2$, then $d_{\mathrm{hom}}(C) = pd_2$. $\square$

Example 5.4. In $\mathbb{Z}_4[x]$, $x^7 - 1 = f_1 f_2 f_3$, where

$$f_1 = x - 1, \qquad f_2 = x^3 + 2x^2 + x - 1, \qquad f_3 = x^3 - x^2 + 2x - 1.$$

Let $C = \langle f_1^3 f_2\rangle$ be the negacyclic code over $\mathbb{Z}_4$ of length 14. Then from Lemma 5.2 we have $\mathrm{Res}(C) = \langle \bar{f}_1^2 \bar{f}_2\rangle$ and $\mathrm{Tor}(C) = \langle \bar{f}_1\rangle$. They are both binary cyclic codes and have parameters $[14, 9, 4]$ and $[14, 13, 2]$. By Theorem 5.3 and Corollary 4.7, the Gray image $\phi(C)$ of C is a $(28, 2^{22}, 4)$ binary code, which is an optimal code.

Example 5.5. In $\mathbb{Z}_9[x]$, $x^4-1=f_1f_2f_3$, where

$$f_1=x-1, \qquad f_2=x+1, \qquad f_3=x^2+1.$$

Let $C=\langle f_2^2 f_3\rangle$ be the $(1+3\lambda)$-constacyclic code over $\mathbb{Z}_9$ of length 4, where $\lambda=1$ or 2. Then $\mathrm{Res}(C)=\langle \bar{f}_2\bar{f}_3\rangle$ is a $[4,1,4]$ ternary cyclic code, and $\mathrm{Tor}(C)=\langle \bar{f}_2\rangle$ is a $[4,3,2]$ ternary cyclic code. Thus, $\phi(C)$ is a $(12,3^4,6)$ ternary code, which is an optimal code.

6. Conclusion

In this paper, we have established the structure of $(1+\lambda p)$-constacyclic codes of length p^s over $GR(p^m,a)$, where λ is a unit of $\mathbb{Z}_{p^m}$. With the help of this structure, we have classified all $(1+\lambda p)$-constacyclic codes over $\mathbb{Z}_{p^m}$ for an arbitrary length. It would be interesting to study other constacyclic codes over $\mathbb{Z}_{p^m}$ and their images under a Gray map.

Acknowledgment

The authors would like to sincerely thank the anonymous referees who gave many helpful comments and suggestions to create an improved version.

References

[1] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Discrete Appl. Math. 128 (2003) 27–46.
[2] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE Trans. Inform. Theory 49 (6) (2003) 1417–1424.
[3] H.Q. Dinh, Negacyclic codes of length 2^s over Galois rings, IEEE Trans. Inform. Theory 51 (12) (2005) 4252–4262.
[4] H.Q. Dinh, Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$, IEEE Trans. Inform. Theory 53 (1) (2007) 147–161.
[5] H.Q. Dinh, On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions, Finite Fields Appl. 14 (2008) 22–40.
[6] H.Q. Dinh, S.R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (8) (2004) 1728–1744.
[7] S.T. Dougherty, S. Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, Des. Codes Cryptogr. 39 (2006) 127–153.
[8] S.T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13 (2007) 31–57.
[9] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36,3^{12},15)$ codes, IEEE Trans. Inform. Theory 45 (7) (1999) 2522–2524.
[10] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (2) (1994) 301–319.
[11] S. Ling, T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592–2605.
[12] B.R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.
[13] A. Sălăgean, Repeated-root cyclic and negacyclic codes over finite chain rings, Discrete Appl. Math. 154 (2006) 413–419.
[14] H. Tapia-Recillas, G. Vega, A Generalization of negacyclic codes, in: Proc. Int. Workshop on Coding and Cryptography, WCC 2001, Paris, France, 2001, pp. 519–529.
[15] H. Tapia-Recillas, G. Vega, Some constacyclic codes over $\mathbb{Z}_{2^k}$ and binary quasi-cyclic codes, Discrete Appl. Math. 128 (2003) 305–316.
[16] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (7) (1999) 2527–2532.
[17] J. Wolfmann, Binary images of cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 47 (5) (2001) 1773–1779.
[18] S.X. Zhu, X.S. Kai, The Hamming distances of negacyclic codes of length 2^s over $GR(2^a,m)$, J. Syst. Sci. Complex. 21 (2008) 60–66.
[19] S.X. Zhu, X.S. Kai, Dual and self-dual negacyclic codes of even length over $\mathbb{Z}_{2^a}$, Discrete Math. 309 (2009) 2382–2391.